

National Security Agency/Central Security Service



Adobe ColdFusion Guidance

July 2015 SERIAL # MTB U/OO/802581-15

 $^{\rm 1}$ Adobe $^{\rm @}$ ColdFusion $^{\rm @}$ is a registered trademark of Adobe Systems, Inc.



Adobe ColdFusion Guidance



Overview

Adobe ColdFusion is an application development platform used within the DoD, public and education sectors to quickly develop and deploy web and mobile applications. Since its release, there have been major vulnerabilities identified within different versions with Common Vulnerabilities and Exposures (CVE) ranging from a 2.1 to 10 (maximum risk) using the Common Vulnerability Scoring System (CVSS). The vulnerabilities enable an adversary to exploit the weakness and potentially gain and expand a foothold in the owner's network. To combat these vulnerabilities, a layered security approach is recommended. The approach covers ColdFusion servers and applications, network segmentation via a Demilitarized Zone (DMZ), and credential management.

ColdFusion Servers and Applications Guidance

The following mitigations are recommended to properly secure the applications and servers:

- Ensure all servers running Adobe ColdFusion are configured using Adobe ColdFusion Lockdown Guide, which can be found on Adobe's website:
 www.adobe.com/support/coldfusion
- Ensure all application code has been developed in a manner consistent with the techniques described in the *Adobe ColdFusion Developer Guide*, also found at the above link.
- Ensure patching is up-to-date and maintained.
- Upgrade to the highest feasible ColdFusion version, currently version 11.
- Track software vulnerabilities identified by United States Computer Emergency Readiness Team (US-CERT) in the National Vulnerability Database (NVD) and, for DOD, of Information Assurance Vulnerability Alerts (IAVAs) identified by U.S. Cyber Command.
- Run the ColdFusion server as a non-administrative user to reduce the actions that can be performed if it is compromised.
- Enforce application whitelisting on servers to prevent malware from running even if the server software becomes compromised.
- Employ a Host Intrusion Prevention System (HIPS) on the server to prevent malicious behaviors and restrict the actions various software on the server can perform.

DMZ Architecture and Configuration Guidance

It is recommended that ColdFusion applications on public-facing servers reside within a DMZ, which is the perimeter network subnet logically between internal and external networks. The DMZ is the area where services, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS) servers, are hosted. The DMZ enforces the internal network's Information Assurance policy for external information exchange and provides external, untrusted sources with restricted access to releasable information. In simplest terms, a DMZ is a broker between external and internal networks and shields the internal network from outside attacks.



Adobe ColdFusion Guidance



The following mitigations are recommended to properly secure the DMZ:

- Set up a Dual Firewall Architecture DMZ, physically or logically. The "perimeter" firewall filters all traffic into the DMZ and an "internal" firewall filters all traffic from the DMZ to the internal network. If the Dual Firewall Architecture is set up logically, then a next-gen firewall should be used with port security and rule sets to direct traffic.
- Utilize a Web Application Firewall (WAF) and/or Reverse Web Proxy (RWP) to further analyze and filter connections to servers in the DMZ.
- Configure the "perimeter" firewall to send all traffic to services in the DMZ only. No Internet traffic should bypass the DMZ. No traffic should connect directly from the external network to the internal networks. All public-facing services should be migrated to the DMZ.
- Configure the "internal" firewall to only accept traffic from necessary DMZ services. All other traffic should be denied. Also set up the "internal" firewall to perform Network Address
 Translation (NAT) so internal IP addresses are not directly addressable from the Internet. If resources permit and high security is needed, procure the "perimeter" and "internal" firewalls from different manufacturers to reduce the chance of a common vulnerability.
- Only employ components that serve external functions (i.e., web servers, mail services, and public FTP servers). The DMZ should not host databases or other services that are only accessed from the internal network or sensitive user files. The components in the DMZ should have a separate addressing scheme than the internal network.
- Limit trust between components in the DMZ and components on the internal network.
 Administration protocols should be blocked from entering the internal network from the DMZ and external networks.
- Use separate Active Directories and Domain Controllers from the internal network.
- Use an out-of-band (OOB) network (if possible) to manage devices and servers in the DMZ and restrict them to only accept management connections from the OOB.

Credential Management Guidance

The DMZ, where Adobe ColdFusion resides, is a particularly vulnerable segment of the network when it is public-facing. It must be locked down to the highest level of security, most especially for the protection of credentials.

The following mitigations are recommended to properly protect the credentials:

- Assign unique passwords to the default local administrative accounts on each platform in the DMZ. Ensure that manufacturer default accounts and passwords are changed on all equipment, especially on network infrastructure equipment.
- Limit administrative access to a small number of dedicated administrative workstations, preferably within an OOB, and enforce this with network and client level access controls. Audit and log any remote administration activity.



Adobe ColdFusion Guidance



- Use least privilege principles when assigning rights to administrative accounts in the DMZ.
 Create and use separate, unique administrative accounts for the DMZ. Do not use administrative accounts for non-administrative activity, especially web browsing or email. Audit and log the use of administrative credentials in the DMZ.
- Use multi-factor authentication to administer devices within the DMZ, and, if feasible, use multi-factor authentication for access to sensitive data within the DMZ.
- Disallow or severely restrict trust relationships between the internal network and the DMZ, so that the DMZ and DMZ credentials are untrusted on the internal network. Do not allow bidirectional trust relationships with the less trusted DMZ.

Conclusion

This guidance provides the foundation for configuring and implementing best practices on servers running Adobe ColdFusion. To ensure adequate protection on servers it is imperative that proper patching and configuration, DMZ segregation, and credential management are effectively implemented. Although this adversarial threat is growing each day, applying these mitigations will go a long way in further protecting your network against critical vulnerabilities affecting Adobe ColdFusion servers and their applications.

Disclaimer of Warranty and Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact Information

Industry Inquiries 410-854-6091 bao@nsa.gov

Client Requirements And General Information Assurance Inquiries

IAD Client Contact Center 410-854-4200 email: IAD_CCC